Exporting and Restoring the System Configuration

Introduction

You can export and save your system configuration and restore earlier versions of your configuration on the General Settings page.

When you backup the system configuration, Proventia Network ADS saves configuration in the following way:

System Configuration	Saved Format or Location
Group objects	Exports it as a CSV file.
Port objects	Exports it as a CSV file.
Notification objects	Saves settings from the Notification Object Configuration page.
Time objects	Saves settings from the Time Object Configuration page.
Services	Saves the settings from the Services page
All alerting and policy configuration	Saves the alerting settings from the Policy page (Built-in behavior, ATF, and user-defined).
Firewall configuration	Saves settings from the Worm Protection Settings page.

Table 28: *Saved system configuration*

Downloading backup configuration

To save the most recent automatically-created backup to your local computer:

- Click DOWNLOAD LAST DAILY BACKUP.

You can also save a file that contains a snapshot of the current system configuration.

- Click GENERATE AND DOWNLOAD BACKUP NOW.

  The system creates a snapshot of the configuration and saves it to the location you specify.

Importing the backup system configuration

To revert to a saved version of the system configuration:

1. Do one of the following:
   - Type the file name in the box.
   - Click **Browse**, and then select the configuration file.
2. Click IMPORT
3. Follow the instructions displayed to restart the Analyzer and save the updated configuration.

Rebooting after importing

When you import a configuration file, the system displays a message with instructions for restoring the configuration output. You must do this manually in the CLI because when you update the configuration, you need to reboot the Analyzer.

Reference: See the *Proventia Network ADS Advanced Configuration Guide* for information about the CLI and instructions for how to reboot the Analyzer

Example message

The following shows an example of the type of message ADS displays when you import a configuration file:

To restore users and ADOS config, please run the following command at the cli prompt: `conf import disk:ads_3.5_config_2006-03-07`.

After the machine reboots, please run: `services ads start`.

Chapter 13

Configuring Services

Overview

Introduction

This chapter explains what the services are, how Proventia Network ADS uses these settings, and how to add and edit services.

User Access on the Services page

Administrators can perform all actions described in this chapter. Analysts and users can view the services but cannot change them.

In this chapter

This chapter contains the following topics:

About the Services Page

Introduction

Use the Services page to map names of services to protocols/ports. Defining custom services allows you to designate certain non-standard ports as ports on which a service is listening. When Proventia Network ADS determines which end of a connection is the client and which is the server, it consults the services table to help make the determination.

Services page layout

The Services page is divided into two panes. The upper pane shows the table of currently configured services, and the Add A Service pane allows you to add new services.

Navigating and searching on the Services page

You can search for a protocol, port, or service name or see examples of search entries. Standard navigation and searching practices apply on the Services page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Services table

The Services table shows the Proventia Network ADS preconfigured services and all of the services users add. The table shows the following information for each service:

Column	Description
Protocol	The name of the protocol.
Port/ICMP Type	A list of the configured ports, or ICMP types for ICMP services.
Name	The name of the service.
Selection check box	Use to select specific services to delete.

Table 29: *Services table*

Configuring Services

Introduction

Add new services in the Add a Service pane. You can add new TCP, UDP, or ICMP services. If there are many configured services, you might need to scroll down to see this pane.

Adding services

To add a new service:

1. Type the protocol name or equivalent number in the **Protocol** box.

   Note: This must be for a TCP, UDP, or ICMP service.
2. Type the corresponding port number or ICMP type if you entered ICMP as the protocol, in the **Port/ICMP Type** box.
3. Type a description that identifies the service in the **Name** box.
4. Click **ADD**.

   Proventia Network ADS displays the new service in the services table.

Exporting service files

You can export the services file for the built-in services to provide you with an example of the file format. The services file is a tab-delimited text file that follows the RFC1700 format.

To export the service file:

1. Click **EXPORT**.
2. Specify how you want to save or open the file, according to the choices your browser displays.

Uploading service files

You can add a file exported from a different Proventia Network ADS machine that contains service listings.

To upload a file:

1. Do one of the following:
   - Type the file name in the box
   - Click **Browse**, and then select the file to be included.
2. Click **UPLOAD**.

   Caution: If you upload a new file, Proventia Network ADS overwrites the existing service information, and you will lose the information in your original file.

Editing services

You can edit an existing service by changing the service name. To edit a service:

1. Type the new name in the **Name** box on the service row.
2. Click **UPDATE**.

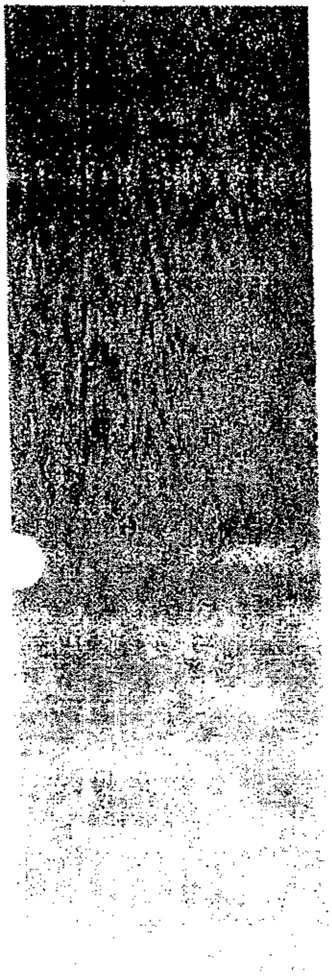
Deleting services

To delete a service:

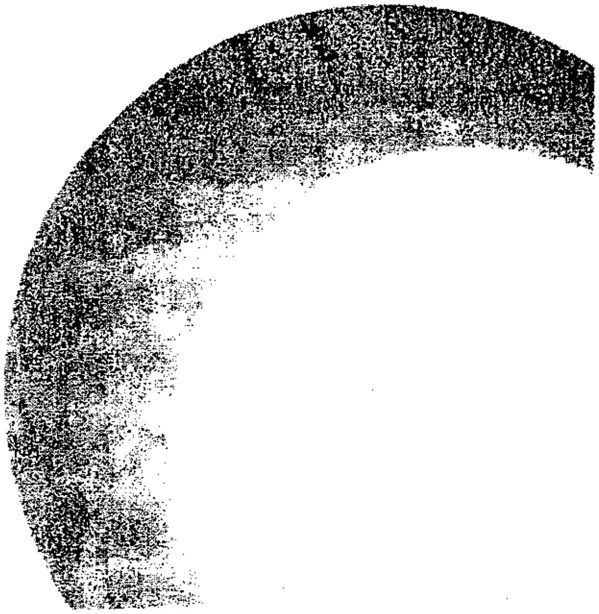
- Select the check box on the service row you want to remove, and then click **DELETE**.

INTERNET
SECURITY
SYSTEMS®

Part III



Using ADS



Chapter 14

Searching Traffic

Overview

Introduction

Use the Explore page to search the traffic on your network, and then create a rule based on the types of traffic the system displays. This topic discusses the various ways you can search the traffic database and how you can act on the results.

User access

Administrators and analysts can perform all actions described in this chapter. Users cannot create rules or make groups from the Explore pages. The buttons for creating group objects and rules do not appear on the pages for users.

In this chapter

This chapter contains the following topics:

About the Explore Page

Introduction

Use the Explore page to search the network traffic database for specific types of traffic and then refine your search, or to create group objects and rules to tune your network policy.

Explore page description

The Explore page initially displays a time series graph that shows all network traffic over the last day and the corresponding traffic in the Traffic data table. The page provides tabs to the Flows and Host Relationships pages where you can see additional views of traffic data. If you enter search values in the Search box, this page displays a description of the search values to help identify the traffic displayed.

Navigating on the Explore page

You can use the various navigation icons to change the view and move through the pages of traffic data.

Reference: See "Using Navigation Controls" on page 14 for these instructions.

Viewing the Traffic table

The Traffic table shows traffic information for all of the clients, servers and services Proventia Network ADS sees. By default, it shows the refined by the Services column.

The traffic table shows the following columns of information:

Column	Description
Client	The gross aggregates of the involved client netblocks (initially displayed as an expansion button). Refine by Client or expand a row to see the information.
Num	The number of individual entries (for clients and servers) that ADS has seen under this aggregate. **Example:** If aggregate 10.0.1.0/24 represents 255 hosts, but the system only observes 72 of them as active, it would display 72 in this column. If you click the 72 link, you navigate to the Host Detail page that shows these 72 hosts.
Server	The gross aggregates of involved server netblocks, initially displayed as an expansion button. Refine by Server or expand a row to see the information.
Service	The gross aggregates of involved services.
Num	The number of distinct services under each aggregate, as a link to the Detail page that lists all services seen and the port objects to which they belong.
Bytes	The total amount of rule-matching traffic the client or server sent or received.
bps	The rate of the rule-matching traffic the client or server sent or received.
Percent	The total percentage of rule-matching traffic the client or server hosts within the aggregate sent or received.
Client Groups	All of the group objects the hosts in the block belong to, when the Server column is expanded. The system displays each group name as a link to the Edit Group Objects page.
Server Groups	All of the group objects the hosts in the block belong to, as a link to their Edit Group Objects page.

Table 30: *Explore traffic data table*

Changing the refine view

The traffic table initially shows the expanded service column. You can change the refine view of the traffic table to see either the expanded Clients or Server columns.

To change the refine view:

- Select the view from the **Refine by** list.

  The system redisplays the page with the selected column expanded.

Navigating to other pages from Explore

You can navigate to pages that allow you to see different views of the traffic data from Explore tab. These are as follows:

Page	How to get there	Function
Rule Editor	Click the New Rule button.	Allows you to create and edit rules for behaviors.
Entity Info	Click the entity icon, and then choose the info link.	Allows you to see detailed data for a chosen entity.
Flows	Click the Flows tab.	Shows the traffic flows that make up the traffic.
Host Relationships	Click the Host Relationships tab.	Shows how a certain host or service is used by others in your network.

Table 31: *Navigation on the Explore page*

References

- See "Creating and Editing Rules" on page 117.
- See "Viewing Entity Information" on page 137.
- See "Viewing Traffic Flows" on page 106.
- See "Viewing Host Relationships" on page 104.

Searching Traffic

Introduction

This topic describes the various ways you can search the traffic database.

Methods of searching

There are multiple ways you can search the traffic database and change the view of the traffic Proventia Network ADS displays:

- By specifying the clients, servers, and services you want to see and the direction of the traffic between them.
- By entering a PFCAP expression for the system to match.
- By changing the refine view.
- By expanding listed client, server, and service aggregates.
- By viewing the relationships between network objects.
- By viewing all of the flows for the traffic you searched for.

Using the graph controls

When you update the traffic you search for, the system automatically updates the graph to show the new traffic. You can change whether you view the traffic as a time series graph or as pie charts.

To change the graph type:

- Select the graph type from the list in the **Graph Controls** box.

  The system updates the view.

Searching by specifying hosts and services

You can search for traffic for specific clients, servers, or services or any combination, and then choose whether you want to see traffic from one aggregate to another or see the traffic between them. Use the More links below each box to see examples of the entry format.

To specify hosts:

1. Type the client as an IP address, CIDR, IP range, or group object name in the **Clients** box.

   When entering IP ranges, you cannot enter spaces between the hyphen and the address.
2. Type the server as an IP address, CIDR, IP range, or group object name in the **Server** box.
3. Type the service as a name, number, or range in the **Service** box.
4. Click **SEARCH**.

   The system redisplays the page with the updated traffic table and the search value as the page name.

Searching with PFCAP expressions

The search format icon allows you to change the way you search for matching traffic. By default, the system displays Client, Server, and Service lists that you can choose from. The expression box allows you to type values that correspond to data in the table that you want the system to match.

To search using an expression:

1. Click the search format icon to toggle to the search expression box.
2. Type the values you want the system to match.

   Enter IP addresses, CIDR addresses, group object names, or case-insensitive descriptive text.

   Reference: See Appendix A, "Using PFCAP Expressions" for additional information and examples.
3. Click the More link to see additional examples of expression formats.

   Note: You can enter a name that contains spaces enclose the name in quotes, but you cannot enter names that contain underscores (_).
4. Click **SEARCH.**

   The system redisplays the page showing all matching values (OR, not AND) with the corresponding page title.

Using timeframes to search

The clock icon allows you to change the type of time frame the system uses to match and display traffic. When you click the icon, the system toggles between the time frames.

An example of the three types of time frames is shown in Figure 2 on page 17.

The following table describes the types of time frames and how you can specify the time frames.

Timeframe	Shows	How to specify the time
Last	Traffic for the last `time period.`	Select from the list of time frames that range from 15 minutes to 1 year.
During	Traffic for the specific time period, starting from the specific time.	Select from the list of time periods. and then enter a start time.
Between	Traffic for a range of time.	Enter a start time and an end time.

Table 32: *Timeframe options*

Searching with the Last timeframe

To search for traffic for the last period of time:

1. Click the clock icon to toggle to the **Last** time frame.
2. Select the amount of time you want to see the traffic for from the **Last** list.

   Options range from the 15 minutes to the last two weeks.
3. Click **SEARCH.**

Searching with the Duration timeframe

To search for traffic that occurred for a specific duration:

1. Click the clock icon to toggle to the **Duration** timeframe.
2. Select the month, day, and year that you want the time to begin from the **Starting at** list.
3. Type the hour and minutes you want the time to begin in the format HH:MM, and then select AM or PM.
4. Click **SEARCH.**

Searching with the Between timeframe

To search for traffic for a range of time, you must first set the start time:

1. Click the clock icon to toggle to the **Between** timeframe.
2. Select a month from the list.
3. Type a number that represents the corresponding day of the month.
4. Select the year from the list.
5. Type the hour you want the range to begin, in the format of HH:MM, and then select **AM** or **PM**.

   Note: If you enter hours as a 24-hour period (for example, 13:00), the system ignores the AM/PM box.
6. Repeat Steps 1 through 4 to set the end time.
7. Click **SEARCH.**

   The table updates to show traffic for the time period.

How to update your search

You can update your search without re-entering another search value by limiting your search to specific clients, servers, or services. Proventia Network ADS shows the rows in the Client, Server, and Server columns as links. Some of these contain an info icon that links to different views of the traffic data for that client, server, or service. Some of these allow you to drill into and some allow you to drill out of the host and service information from the pages on the Explore tab (Explore, Host Relationships, and Flows).

How links work on the Explore page

Links apply only to the specific object. Table 33 shows a description of all options. Note that they all do not appear on all pages or for all columns of information. If you click a link, the system navigates to the linked location, ignoring any selected rows.

Example: If you search for a service, and you click on a host name link, the search narrows to show only how the host uses the service. If you then click Limit to for that host, you'll get a search containing only the host (the service has been removed).

Link descriptions

The following table shows the links and what they do on the Explore page:

Link	Description
Aggregate or host name link	Shows all instances of that aggregate and how it talks to other objects on your network.
Connect to	Connects you to the Web address of the host displayed.
Limit to	Limits the search to only those hosts, shows only the selected aggregates, all others disappear from the table.
Info	Navigates to the Entity Info page, which shows the service this host or group is a client of, server of, service of, and shows any alerts it is involved in, and any SiteProtector events.
Explore	Navigates to the Explore page and displays the search results for that host.

Table 33: *Link descriptions*

Viewing additional details

To view additional details:

1. Do one of the following:
   - Click the host or service link.
   - Click the info icon, and then select the link from the pop-up window for the view you want.
2. Repeat Step 1 to see the next level of details, if applicable.
3. Click your browser's back button to return to the prior page.

References

- See "Viewing Entity Information" on page 137 for information about the Info page.
- See "Viewing Traffic Flows" on page 106 for information about the Flows detail page.
- See "Viewing Host Relationships" on page 104 for information about the Host Relationships page.

Searching and Viewing Aggregated Data

Introduction

This topic explains how to view the aggregated traffic rows in the traffic table and the ways you can search to find specific traffic.

Searching by expanding aggregated rows

You can expand any aggregated client, server, and service rows to see the hosts and services that make up the aggregated statistics. Initially, the system displays the traffic table expanded by (Refine by) Service. The Client and Server columns are collapsed and display an expansion (plus sign +) button. When you click the expansion button, the system expands the row to show the next level of aggregates. You can continually expand all collapsed rows to select either a single host or an aggregate row, which includes all members that make up the aggregate.

Searching over aggregated group objects

You can filter the search results by choosing a group object for Proventia Network ADS to use when it aggregates traffic. When you aggregate by a specific group object, the system only looks at the traffic over that group space instead of over the whole network (Auto). You can only aggregate by a group if the Report Aggregate check box for the group on the Edit Group page is selected.

Reference: See "Using the report aggregate option" on page 51.

Example: If you have a group object that contains five CIDR blocks and has the Report Aggregate setting selected on the Edit Group Object page, the object appears as a choice in the Aggregate by list on the Explore page.

If you select the group to aggregate by when you search, the system aggregates traffic up to only the members of that group object and only displays traffic results related to that object. It shows the traffic breakdown for those five CIDR blocks in the Traffic table that are part that group object, each block's associated traffic, and an Other category that includes those that contributed to the traffic total, but weren't explicitly one of the five members.

Important: If you search over a network that the group object is not a part of, the system does not show any traffic from that group in the search results, just the Other category.

When group members are other groups, the system displays their assigned group names in the table instead of their IP addresses.

Viewing aggregated data

When you search for specific traffic, the system shows the results in aggregated data tables. The top line shows the aggregate that represents all traffic seen, with each following line showing more specific data. Each row shows the bytes, which is the total count of bytes seen for that row for the entire aggregate, and the bps, which is the rate at which traffic is flowing. The percentage it displays represents the %bps of the total, meaning that there is an overall amount of traffic flowing by for the clients, servers and services.

Example of aggregated data

Table 34 shows example search results for two appliances (10.0.1.116 and 10.0.1.96) included in an aggregated row for the 10.0.1.0/24 network.

Client	Bytes	bps	% bps
10.0.1.0/24	100 K	100 bps	100 %
10.0.1.0/25	100 K	100 bps	100 %
10.0.1.96/32	75 K	50 bps	50 %
10.0.1.116/32	25K	50 bps	50 %

Table 34: *Aggregated data example*

This table shows 10.0.1.0/24 is an aggregate that covers all the traffic in this row and the range of IP addresses 10.0.1.1-10.0.1.255. Both of the appliance addresses (10.0.1.116 and 10.0.1.96) are in this range. Therefore, the bps and %bps are both 100.

The second aggregate, 10.0.1.0/25, covers the range of IP addresses 10.0.1.1-10.0.1.128. Both appliance addresses are also in this aggregate, so the system again displays 100 for the bps and %bps.

The rows with the two /32 (single IP) addresses show the actual appliance traffic. The 10.0.1.96 appliance is seeing a higher byte count (75k), but both appliances have traffic that is flowing at a 50bps rate.

Viewing Host Relationships

Introduction

The Host Relationships page shows you the relationships between clients and servers for the traffic you specify. The Host Relationships view allows you to see the relationships between objects on your network. This page shows the detailed information for the traffic between the selected network objects, including the client, server, service, and then the total traffic and traffic rates between those objects.

Navigating to the Host Relationships

Navigate to Host Relationships from either the Explore page or the Flows page by clicking the Host Relationships tab. If the search box on the previous page contains values, those are carried over and the Host Relationships page shows the relationships within those search parameters for the selected time period.

Example: If you view traffic on the Explore page for the last hour, when you navigate to Host Relationships, it also shows the relationships for the last hour.

Navigating on the Host Relationships page

Standard navigation, and time controls apply on the Host Relationships page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12 for instructions.

The Details table

The Details table shows the following relationship details:

Column	Description
Client	The Host IP address and name, if known.
Server	The server IP address and name, if known.
Service	The service that the two hosts communicate over.
Bytes	The amount of traffic flowing between these hosts.
Bps	The rate at which traffic is flowing between these hosts.

Table 35: *Traffic details table*

Searching on host relationships

From Host Relationships you can further constrain the results to a specific host, search for a different time period, search over a less or more specific CIDR block. By default, each host is shown as a /32 to show the most specific information.

To change the search values:

1. Type new or additional values in the Search text box.

   Enter any CIDR address or group name and enter any specifiers, such as "src" or "dst," or click More to see more examples of the search entry format.
2. Select the time period during which you want to see the relationships.

   Reference: See "Using timeframes to search" on page 99 for these instructions.
3. Select the netmask you want the system to use for showing clients from the **Client Mask** list.
4. Select the netmask you want the system to use for showing servers from the **Server Mask** list.

5. Click **SEARCH**.

   The updated Details table appears.

Viewing additional host relation details

You can expand and pivot the view of the relationship details shown on the Host Relationships page.

Reference: See "How to update your search" on page 100 and "Using info icons" on page 15.

Exporting host relationship details

You can export the details from the table as a CSV file. Exporting this information can help you with cleanup following a worm infection or other type of attack, or you might want to use this information for compliance auditing, or in certain types of reports.

To export the file:

1. Click **EXPORT**.
2. Specify how you want to save or open the file, according to the choices your browser displays.

Viewing Traffic Flows

Introduction

Proventia Network ADS saves a record of all ongoing traffic in a rotating flow log as it watches your network. The Flows page shows these flows for specific clients, servers, or services, or for all of the traffic data.

Navigating to the Flows page

You can navigate to the Flows page from any of the pages within the Explore tab or from the Alert Detail page. If the search box contains values, those are carried over and the Flows page shows the flows within those search parameters.

Example: If you are viewing traffic on the Explore page for a specific service (TCP port 22) and click the Flows tab, the Flows page shows you all of the TCP port 22 flows. The filter at the top of the page shows (22) indicating those are the flows displayed.

If you navigate from the Alert Detail page, the Flows page also shows the rule name as a link to its Event Details page.

Navigating on the Flows page

Standard navigation, and time controls apply on the Flows page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12 for instructions.

Details table

The Details table shows the following flow information:

Column	Description
Client	The IP address and possibly the host name of the client.
Server	The IP address and possibly the host name of the server.
Service	The service protocol or destination port (TCP/22, UDP/514, etc.)
Sport	The source port number or Any.
Sflags	The source flags.
Dflags	The destination flags.
Start	The time the flow started.
Dur	How long it took for the flow to be sent and received (duration).
Server	The server IP address and name, if known.
Service	The service that the two hosts communicate over.
Bytes	The amount of traffic flowing between these hosts.
Bps	The rate at which traffic is flowing between these hosts.

Table 36: *Flow Details table*

Note: The allotted disk space to store flow log information is a fixed number. When the log reaches its maximum size, Proventia Network ADS discards the oldest entries to make room for newer entries.

Searching on the Flows page

On the Flows page, you can search for specific flows and over a different time period. You can also search the traffic database using PFCAP expressions.

To change the search values:

1. Type new or additional values in the search box.
2. Enter any CIDR address or group name and enter any specifiers, such as "src" or "dst," or click the More link to see more examples of the search entry format.
3. Select the time period during which you want to see the relationships.

   Reference: See "Selecting the timeframe" on page 17 for these instructions.
4. Select the client netmask you want the system to use for showing **Clients** from the list.
5. Select the Server netmask you want the system to use for showing **Servers** from the list.
6. Click **SEARCH**.

   The updated Details table appears.

Viewing additional flow information

You can expand and pivot the view of the flow information shown on the Flows page.

Reference: See "How to update your search" on page 100 and "Using info icons" on page 15.

Exporting flow information

You can export the details from the table as a CSV file. Exporting this information can help you with cleanup following a worm infection or other type of attack, or you might want to use this information for compliance auditing, or in certain types of reports. The maximum number of flows you can export is 64,000 rows

To export the file:

1. Click **EXPORT.**
2. Specify how you want to save or open the file, according to the choices your browser displays.

Creating Group and Port Objects from Traffic

Introduction

When you search for traffic on the Explore page, the system displays any traffic that matches the search values you enter. You can create groups from the hosts or services and create new rules for the resulting traffic you see.

Creating group objects

You can make new groups that include any or all of the clients or servers listed in the tables, or add to existing groups. While you can create groups manually on the Group Object Settings page, creating groups from the Explore page allows you to see the traffic that hosts are involved in and then put them in groups according to the way they behave.

Reference: "Adding and Editing Group Objects" on page 51 for more information.

To create a group:

1. Select the check boxes for all of the clients and servers you want to group together.

   Note: When selecting aggregates, the system includes the whole netblock when making groups, not only the hosts represented in the number (Num) column.

2. Do one of the following:

   - Enter a unique name for the group object in the box for a new object.

     Reference: See "Naming group objects" on page 51.

   - Type the name of an existing group object in the box to add the hosts or aggregates to an existing object.

3. Click **NEW GROUP OBJECT**.

   If you are adding members to an existing group object, the system displays a message confirming you want to update the group members, click OK to add the members.

Editing client and server group objects

Each group object listed in the Groups column is presented as a link to its Configure Group Objects page. Use the link to navigate to the edit page to change group object settings.

Reference: See "Adding and Editing Group Objects" on page 51.

Creating new port objects

You can make new port objects that include any or all of the services listed in the tables. While you can create groups manually on the Configure Port Objects page, creating port objects from the Explore page allows you to see the traffic hosts are involved in and then put them in groups according to the way they behave.

Reference: See "Adding and Editing Port Objects" on page 81.

To create a port object:

1. Select the check boxes for all of the services you want to group together.

   Note: When selecting aggregates, the system includes all ports represented by the range when making groups, not only the services represented in the number (Num) column.

2. Do one of the following:

- Enter a unique name for the port object in the box for a new object.

  Reference: See "Naming port objects" on page 81 for a list of characters you can use.

- Type the name of an existing object in the box to add services to an existing object.

3. Click **NEW PORT OBJECT**.

   If the system displays a message confirming you want to update the group members, click **OK** to add the members.

Creating rules from the Explore page

The Explore page displays a Create Rule button for users with administrator or analyst-level privileges. Use the button to navigate to the Rule Editor page.

Reference: See "Creating and Editing Rules" on page 117 for instructions and additional information.

Chapter 15

Managing Policy Rules

Overview

Introduction

This chapter describes how to view event activity, and how to create and edit rules associated with system and user-created behaviors.

User access

Administrators and analysts can perform all the actions described in this chapter. Users can view activity but cannot create or edit rules.

In this chapter

This chapter contains the following topics:

About the Activity Page

Introduction

The Activity page shows the behaviors Proventia Network ADS is monitoring. You can choose to see all behaviors, only those that are currently alerting, or only those on the Watch list, which means they are active, but not alerting.

Navigating and searching on the Activity page

You can search for types or names of behaviors, the behavior creator, or names of groups involved in behavior. Standard navigation and searching apply on the Activity page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Viewing the Activity table

The Activity table shows the following information for each behavior:

Column	Description
Severity	The user-assigned level the system applies when it detects violations of this behavior.
Behavior	The name of the behavior as a link to the Event Details page.
Creator	The user name for user-created rules or ATF or System for behaviors ADS created.
Traffic graph	A mini graph of the traffic for this behavior over the last 24 hours as a link to the Event Details page. Activity in green represents approved traffic and activity in red represents unapproved traffic.
Approved traffic	The average and maximum amounts of accepted traffic (in bps) that the system has detected.
Unapproved traffic	The maximum and average amounts of unapproved traffic (in bps) that the system has detected.
Alerts	A summary message for each alert type that includes the number of times the system detected the alert traffic.
First alert	The time the system first detected alert traffic for the behavior.
Last alert	The time the system last detected alert traffic for the behavior (or Ongoing if it still detects alert traffic).
Selection check box	Use to delete behavior alerts or behaviors on the Watch List.

Table 37: *Activity table*

Changing the Activity table view

You can choose which behaviors you want to see in the Activity table.

To change the view of the Activity table:

- Select the type of behaviors you want to see from the **Display** list.

  The page displays the behaviors that are alerting by default.

Alert maximums

The system logs up to 100,000 alerts per rule and one million alerts total. After the system reaches this limit, it displays a red square in the Alerts column on the Activity page. The system displays a message to remind you that the limit has been reached when you move the mouse over the square. You must delete alerts for the rule before the system can create new alerts.

Deleting behaviors

When you delete a behavior, the system also deletes all existing alerts it generated from the behavior.

To delete behaviors:

- Select the check box in the behavior rule row, and then click **DELETE**.

Rule status

Proventia Network ADS displays automatically-generated rules with either "system" or "ATF" as the creator on the Activity page and in the recent changes tables. When ADS creates a behavior rule, it automatically places it on the watch list. All rules remain on the watch list unless there are alerts associated with the rule. When the system detects traffic that violates the rule, it moves the rule to the Alerts list.

For ATF-generated rules, once the ISS security team no longer deems the behavior a threat, it marks the rule for deletion. If the system does not detect unapproved traffic for 30 days, it deletes the ATF rule upon the next ATF update. If there is a new threat, the ATF creates a new policy rule.

Reference: See "Recreating deleted ATF behaviors" on page 71.

Note: The system automatically deletes system-generated and ATF rules if it has not detected alert traffic for a period of 30 days.

Important: You must configure the system to enforce rules on the Worm Protection Settings page. See "Configuring Worm Protection Settings" on page 73 for these instructions.

Navigating to the Event Details page

The Event Details page shows the details of the event, including a breakdown of all of the alert types that violated the behavior to make up the event.

To navigate to the Event Details page:

- Click the behavior name link.

  The Event Details page appears, showing all alerts.
- You can edit the alert configuration and the rules for the behavior.

Viewing Event Details

Introduction

The Event Details page shows all of the details for a behavior that triggered an event, including all violations to the behavior. You can also search to see specific alert traffic for this event.

User access on the Event Details page

Administrators and analysts can perform all actions described in this topic. Users can view the details but cannot make any changes to rules or ACL numbers.

Event Details page layout

The Event Details page layout varies, depending upon the type of behavior and the violations Proventia Network ADS detects. All Event Detail pages display a stacked traffic graph for the specified time period, data tables for each type of violated alert, and a list of recent behavior changes.

Navigating and searching on the Event Details page

Standard navigation, searching, and time controls apply on the Event Details page. You can also search the traffic database using PFCAP expressions.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12 and "Selecting the timeframe" on page 17, and "Using PFCAP Expressions" on page 151.

Viewing traffic graphs

The system displays a graph of this rule's traffic for the selected time period. By default, it shows the traffic for the last day. You can change the time period the system displays by selecting a different time frame.

Reference: See "Selecting the timeframe" on page 17.

Viewing alerting tables

The alerting tables show each type of alert type for which ADS has detected violating traffic. See "Types of alerts" on page 22 for descriptions of each alert type. While these tables vary depending upon alert type, most of them show the following information:

Column	Description
Severity	The overall severity level of the alert. **Reference:** See "How Proventia Network ADS Determines Severity" on page 60.
Client	The IP address for client and connection violations, and the total number of unique sources for other alerts.
Server	The IP address or total number of unique destinations.
Service	The service that is involved in the alert traffic or the number of unique ports or protocols.
First	The time and date the system first detected traffic that violates this rule.
Last	The time and date the system last detected traffic that violates this rule.
Bytes	The total bytes of the alert traffic.

Table 38: *Alerting tables*

Column	Description
Magnifying glass icon	Links to the Alert Details page for this alert. See "Viewing Alert Details" on page 135.
Selection check box	Use to include rows for accepting or clearing alerts.

Table 38: *Alerting tables (Continued)*

Viewing affected groups

The names of the affected groups are listed above the table with an info icon you can use to navigate to the info page for that group, or to the edit page to change the group object's settings.

Reference: See "Using info icons" on page 15.

Generating ACLs

Proventia Network ADS creates rules for some of the built-in behaviors, like floods. For these behaviors, you can generate ACLs automatically from the Event Details page.

To generate an ACL from an alerting table:

1. Select the check boxes for the alert traffic you want to create an ACL for.
2. Click **GENERATE ACL.**

   The View ACL page appears and displays the ACL rules the system generated.

Reference: See "Viewing ACLs" on page 122.

Clearing alerts

You can clear alerts once you have determined they do not pose a threat to your network. You can clear the alerts displayed in the tables for each alert type. If you clear an alert but do not update the rule, ADS continues to generate alerts for any future violations of the rule that it detects.

To clear alerts:

1. Do one of the following:
   - Select the check box for the alert row that you want to remove.
   - Select the Select All check box at the top of the table to include all alerts on this page.
2. Do one of the following;
   - Click **CLEAR ALERTS** to clear those on this page.
   - Click **CLEAR ALL** to clear all of the alerts across multiple pages.

     The system removes the alerts from the Event Details, the Activity, and the Alert Details pages.

Recent Changes table

The Recent Changes table displays a list of the most recent rule changes for you to reference. See "Viewing recent changes" on page 59 for a description of each column.

To see the complete list of all rule changes:

- Click the Full change log for rule link to navigate to the Log Details page.

Reference: See "Viewing Log Details" on page 132.

Exporting alert information

You can export the details from any of the alert tables as a CSV file.

To export the alert information:

1. Click the Export button above the alerts table you want to export.
2. Select the location to save the file to, according to the options your browser displays.

Navigating to the Info page

You can navigate to the Info page for clients and servers that are listed in the table.

To navigate to the Info page:

- Click the IP address or hostname link of the client or server.

  Reference: See "Viewing Entity Information" on page 137.

Navigating to the Rule Editor page

Each behavior name in the Alerting column in the Recent Changes table is presented as a link to the Rule Editor page.

To navigate to the Rule Editor for that behavior:

- Do one of the following:
  - Click the behavior name link.
  - Click EDIT RULE.

  The Rule Editor page appears where you can change all of the rule settings, including alerting settings, for that behavior.

  Reference: See "Editing rules" on page 118.

Navigating to the Alert Details page

To navigate to the Alert Details page:

- Click the magnifying glass icon on the alert row.

  The Alert Details page for the specific alert appears.

  Reference: See "Viewing Alert Details" on page 135.

Navigating to the Alert Configuration page

For flood behaviors, the Event Detail page also displays the Alert Configuration table below the alert type tables. The Alert Configuration table shows the current alerting settings ADS is applying to the behaviors. These are the default settings configured on the Policy Settings page, unless those settings have been overridden for a specific behavior or rule from an Event Details page.

To override the default settings and apply new settings to this behavior:

- Click EDIT ALERT CONFIGURATION.

  The Alert Configuration page for this behavior appears, and displays the current settings.

  Reference: See "Configuring Alerting Settings for Built-in Behaviors" on page 65.

Creating and Editing Rules

Introduction

You can create a rule for behaviors by defining acceptable use and then applying alerting settings on the Rule Editor page.

User access for the Rule Editor page

Administrators and analysts can create and edit rules as described in this topic. Users do not have rule editing privileges and cannot navigate to the Rule Editor page.

Rule Editor page layout

For new rules, the Rule Editor page shows a pane in which you designate the traffic you want Proventia Network ADS to watch. For existing rules, the Rule Editor page shows the configured name, description of the traffic the system is watching, and the alerting configuration. It also shows any alerting or unapproved traffic the system has detected that violates this rule. If the rule has been violated by more than one alert type, you can pivot the view to see the violating traffic for each alert type.

Reference: See the topic "Viewing alerts on the Rule Editor page" on page 118 for additional information.

Navigating and searching on the Rule Editor page

Standard navigation and searching apply on the Rule Editor page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Naming rules

When you add a rule, you assign it a name. Choose one that allows you to easily identify it. The following list shows all of the characters you can use in a rule name:

- Any letters (capital or lowercase)
- Any whole numbers (0-9)
- Spaces
- Underscores (_)
- Colon (:)
- Period (.)
- Hyphen (-)
- Question mark (?)
- Pipe (|)
- Parentheses ( )
- Number/pound sign (#)
- Asterisk (*)
- Plus sign (+)
- Equal to sign (=)

Creating a new rule

To create a new rule:

1. Navigate to the Rule Editor page.

   Click **NEW RULE** on the Policy page.
2. Type a name for the rule.

3. In the Description box, type a description that helps identify the rule.
4. In the Traffic to Watch pane, choose one of the following options:
   - **From** to watch traffic in one direction (from A to B)
   - **Between** to watch traffic in either direction.
5. Do one of the following:
   - Type in the IP addresses or CIDR blocks for each entity in the **From** and **To** or **Between** boxes.
   - Click the group selector icon, and then select a group name from the pop-up window for each from/to or between entity.
6. Type the service you want to watch as a port name or number in the **Service** box.
7. Click **CONTINUE**.

   The Rule Editor page refreshes and displays the page layout for existing rules and shows all traffic that matches the rule. From here, you can edit the rule to accept behaviors for the traffic the system is watching and edit the rule's alerting configuration.

   Reference: See "Editing rules," below.

Viewing alerts on the Rule Editor page

The Define Acceptable Use pane shows the alerts that violate a rule, or the unapproved traffic for newly created rules the system is watching but that don't have alerting configured yet. The system creates an alert table for each type of rule violation.

For each type of alert table, the Rule Editor displays the following columns of information. The information varies depending upon the alert type.

Reference: See "Viewing alerting tables" on page 114 for a description of the table columns.

Changing the activity view

To change the view to see each table:

1. Select the type of activity you want to see from the **Show** list.
2. Select how you want the system to display the alerts from the **As** list.

   The pane displays the corresponding table.

Editing rules

You can edit system and user-created rules by adding approved traffic to the rule and updating alert configuration. Any traffic you do not explicitly accept is considered unacceptable. In this way, your overall network policy continually evolves.

You can either view unapproved traffic or alerts, depending upon the rule, and then add approved connections to the rule. For newly created rules, the system will not create alerts, because you have not yet defined alerting. The unapproved traffic option optimizes the workflow because it allows you to query the traffic and accept traffic from the results, rather than adding approved clients manually. After you accept the connections you want to include, from the results you see, you can turn on alerting to find violators.

You can accept traffic for specific hosts, for groups, or for a covering aggregate. When you accept traffic, the system updates the ACL rules and refreshes the page to show only the new violators.

If you accept traffic and enable enforcement, Proventia Network ADS sends the corresponding ACLs to your configured firewalls and switches and blocks violating traffic.

Editing rule from traffic

To edit rules from the detected traffic:

1. Select one of the following from the **Show** list:
   - Alerts
   - Unapproved Traffic
2. Select the type of alerts you want to see from the **As** list.
3. Enter search values in the box to filter the results.
4. Do one of the following:
   - Select specific rows for the traffic that you want to approve, and then click **APPROVE.**
   - Click **APPROVE ALL.**

   Note: This option approves all of the alerts across multiple pages.

Editing a rule by adding approved traffic

To edit a rule by adding new approved traffic:

1. Select the option for the alert type you want to approve from the **Approve New** list:
   - Clients
   - Servers
   - Services
   - Connections
   - Host Pairs
2. Select a client and server by using one of the following methods:
   - Type the client or server name, IP address, or CIDR block.
   - Click the group icon and select a group from the choices in the pop-up window.
3. Type the service as a port number or name in the **Service** box.
4. Click **ADD.**

Clearing alerts

When you clear alerts, the system removes them from the alert count totals on the Activity page.

To clear alerts:

- Do one of the following
  - Select the check boxes for the alerts you want to clear, and then click **CLEAR.**
  - Click **CLEAR ALL** to remove all alerts in the table.

Reference: See "Alert maximums" on page 112.

Configuring rule alerting

Every Proventia Network ADS rule has its own associated alert configuration. Each time you create a rule, the system applies the built-in behavior alerting configuration to it, unless you have specified other settings that apply to a particular rule. You can define how you want Proventia Network ADS to create events and send alerting notifications on the Alert Configuration page.

Reference: "Adding or editing alerting settings" on page 67 for instructions.

Navigating to the View ACL page

You can view the ACLs that Proventia Network ADS creates when you define the acceptable use, and then copy and paste these formatted rules onto your enforcement devices. For worm behaviors, you can enforce the rules so that Proventia Network ADS updates the ACL and automatically starts filtering out violating worm traffic.

Reference: See "Viewing ACLs" on page 122.

Enforcing Worm Behaviors

Introduction

You can enforce system-generated worm rules, which send the ACLs to your firewalls or switches if you have configured your Proventia Network ADS Analyzers for enforcement. While a regular Activity page shows a breakdown of the accepted and violated traffic, an Activity page for an enforced rule shows the actual traffic Proventia Network ADS accepted and denied. Proventia Network ADS issues alerts when it detects worm policy violations. You can enforce worm policy from these alerts so that the system activates the filter rules, denying the unsafe worm traffic. The filters then block the protocol used by the worm, except for wildcard any-to-server rules, for all legitimate servers on your network.

About automatic enforcement

You can enable Proventia Network ADS to enforce a rule and deny violating traffic automatically when it detects a worm. Before you can enable automatic enforcement, you must configure the worm protection settings. You can enable enforcement either for all worm behaviors or for a specific rule. By default, Proventia Network ADS creates server-only rules when it generates rule sets for worm behaviors. You can change your enforcement preferences on the Worm Protection Settings page.

Procedure

To enforce a worm rule:

- Do one of the following:
  - On the Rule Editor page, verify the **Enable Enforcement** check box is selected on the Rule Editor page, and then click **DONE**.

    Important: If the Enable Enforcement check box is not available, it means worm protection settings are not configured.

    Reference: See "Configuring Worm Protection Settings" on page 73 for these instructions.
  - On the Event Details page, click **ENFORCE**.

The system starts filtering any unsafe traffic. You can view the approved traffic and denied traffic and traffic graphs by choosing the policy from the Activity page.

Canceling enforcement

When you stop enforcing a rule, Proventia Network ADS stops blocking denied traffic but continues watching the rules for the behavior and generating alerts when it detects violating traffic.

To cancel enforcement:

- Click **CANCEL ENFORCEMENT** on the Event Details page.

  The system stops automatically enforcing the rules and displays the unapproved traffic in the Alerts tables on the Event Details page.

Viewing ACLs

Introduction

The View ACL page shows all of the ACL rules that Proventia Network ADS creates for a particular behavior from what is defined as acceptable traffic on the Rule Editor page.

Navigating on the View ACL page

Use standard navigation on the View ACL page.

See "Navigating the Proventia Network ADS Web User Interface" on page 12.

User access

Administrators and analysts can view ACLs and update the ACL number. Users can view the ACLs but cannot update the ACL number.

About ACLs

The system displays the behavior name and the ACLs as static text. You can copy and paste the ACL rules from this page onto your configured enforcement devices.

Proventia Network ADS tries to match traffic by going through the list of rules, starting at the top. When it finds traffic that matches a rule, it stops at that point and designates that traffic as accepted or denied, as appropriate.

The following shows an example of the rule format:

```
access-list 100 deny ip host 168.198.1.42 any
```

Editing the ACL number

Proventia Network ADS uses the reserved ACL numbers, configured on the Worm Protection Settings page, when assigning numbers to ACL rules. You can override the number the system uses as the first rule number by choosing another number that falls within the range you assigned on the Worm Protection Settings page.

Procedure

To update the ACL number:

1. Type the number you want the ACL rules to begin with in the ACL Number box.
2. Click UPDATE.

   The system updates the ACL list, starting with the number you entered.

Chapter 16

Monitoring Network and Appliance Status

Overview

Introduction

The Summary page provides an overview of the current state of your Proventia Network ADS deployment, including the historical traffic across your configured devices.

User access on the Summary page

Administrators can perform all of the actions described in this chapter. Analysts and users can search and view the information, but cannot navigate to all of the pages described.

In this chapter

This chapter contains the following topics:

Viewing the Summary Page

Introduction

Proventia Network ADS displays the Summary page when you log on. It shows you the top alert status, system statistics, recent policy changes, and system information. The system displays important status messages at the top of the page, so you know if there are any problems that require immediate attention. These include connectivity problems, RAID failures, enforcement failures, and auto-generated policy notifications.

Summary page layout

The Summary page shows the status summary in a variety of tables and panes. The following table describes each area of the page:

Pane	Description
System response area	Displays any critical messages.
Alerts table	Shows the top alerts the Analyzer has detected.
Network activity	Shows the current network activity in a graph and corresponding table.
Detectors	Shows a count of the types of behaviors Proventia Network ADS is actively watching.
ADS status	Shows the statistics for your Analyzer and Collectors.

Table 39: *Summary page panes*

Searching and navigating on the Summary page

You can search for a rule name, the creator of a rule, or any alert types or groups, or see examples of search entries. Standard navigation and searching applies on the Summary page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Navigation links on the Summary page

You can navigate to the following pages from the Summary page:

To see this page...	Click...
Event Details	the Behavior name link in the Alerts column or the traffic minigraph.
Activity	the links (alerting rules and total) below the Alerts table to see the complete list of alerting rules (or behaviors) Proventia Network ADS is currently monitoring.
Collector summary	the More button in the ADS status pane.
About page	the Copyright and Legal notices link.

Table 40: *Navigation on the Summary page*

Viewing Alerts on the Summary Page

Introduction

The Alerts table shows a summary of the top alerts the system created for detected behavior violations.

Searching the Alerts table

You can search the system to see particular alerts by entering text that matches any of the values in the data table, such as group names, the creator, or alert types. The system updates the table to show only those alerts that match the search values or all alerts if you do not enter search values.

To search for specific alerts:

1. Enter the search values in the Search box.
2. Click **SEARCH**.

   Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12 for more information about navigating and searching.

Viewing the Alerts table

The table shows alert information that occurred during the last 24 hours. The table includes the following information for each detected alert:

Column	Description
Severity	The relative severity the Analyzer associates with this alert, on a scale from 1-10. 1 is the least severe setting and 10 is the most severe setting. **Reference:** See "How Proventia Network ADS Determines Severity" on page 60.
Behavior	The name of the policy the traffic is violating, as a link to the Event Details page.
Creator	Shows either System, ATF, or the name of the user for user-created rules.
Traffic Over 24 hrs	A mini graph of the traffic for the last 24 hours that links to the Event Detail page.
Unapproved Traffic	The average and maximum rates (in bps) of unapproved traffic for the last 24 hours.
Approved Traffic	The average and maximum rates (in bps) of approved traffic for the last 24 hours.
Alerts	The number of times that rules for this behavior have been violated.
First Alert	The time the system first detected the alert traffic.
Last Alert	The time the system last detected alert traffic or Ongoing if it is currently seeing unapproved traffic.

Table 41: *Alerts table*

Alerting maximums

Proventia Network ADS logs up to one million alerts and 100,000 alerts per rule. After the system reaches either of these limits, it displays a red square in the Alert column header, the number of rules that have reached the limit, and a warning message in the behavior row. When the limits have been reached, you must delete some alerts before the system can create new ones.

Reference: See "Clearing alerts" on page 136.

Viewing all alerting rules

The alerting rules summary row, located below the Alerts table, shows the number of alerting rules displayed that the system has detected over the last 24 hours, the number of alerting rules, and the total number of rules the system is monitoring. The system displays the number of alerting rules and the number of total rules as links to the Activity page that show all rules. You can filter the rules the system displays on this page to only see those currently alerting or those that are on the Watch List.

Reference: See "About the Activity Page" on page 112.

Viewing a Summary of Network Activity

Introduction

The activity section shows the overall network activity level and what the system is currently monitoring.

Network Traffic graph

The Network Traffic graph shows the overall network traffic, in bps (bits per second) for the past 24 hours. You can identify traffic spikes at certain times, and then explore the traffic for those time periods.

Reference: See "Searching Traffic" on page 98.

Network Activity table

The Network Activity table shows the total traffic and number of hosts Proventia Network ADS has detected since it started monitoring your network. The table also shows the number of flows per second and packets per second it is currently detecting.

Detectors table

The Detectors table shows the types of behaviors Proventia Network ADS is detecting and the number that are generating alerts.

Reference: See "Built-in Behavior Descriptions" on page 62 for more information about each type of behavior.

Viewing ADS Status

Introduction

The ADS Statistics section provides a snapshot view of your appliances and the information Proventia Network ADS is collecting and tracking across your network. This topic describes this information.

Last ATF update

The Last ATF update shows the last time (hours and date) your Analyzer retrieved updated information and the Last ATF check shows the last time your Analyzer polled the ATF server to see if there was new information. You can update the ATF interval time and poll the server on the Policy page.

Reference: See "Configuring Active Threat Feed Settings" on page 71.

Last backup

The Last backup shows the time that the system backed up Analyzer data. The Analyzer data is backed up automatically once every 24 hours. You can create a copy of the last backup file or revert to an older saved version.

Reference: See "Exporting and Restoring the System Configuration" on page 87 for a description and instructions.

Total Collectors and flow sources

This section shows you the number of configured Collectors and flow sources. The Collector total includes your Analyzer if it is functioning as a Collector and collecting data from routers or interfaces. If this is the case, the Analyzer name appears in parentheses next to the host name. Flow sources include all configured routers and any interfaces from which the Analyzer is capturing packets.

System messages

The system displays one of the following system messages to describe the appliance status:

Message	Description
All system components are healthy	The appliance is functioning correctly.
Collector *name* is offline	The Analyzer is not receiving heartbeats from the Collector.
Collector *name* is up with errors	The Analyzer is receiving heartbeats, but not functioning optimally (for example, in cases of high memory usage).
Multiple components have problems	There are multiple components with problems.

Table 42: *ADS Status system messages*

System Status table

You can expand and collapse the ADS Status section to display the System Status table. The System Status table shows more information for your Proventia Network Analyzer and for all Collectors. The name of each appliance appears in the table, and includes the Analyzer appliance information if it is collecting flows. This allows you to see how each appliance is performing.

The table displays the following information for each appliance:

Column	Description
Severity	Color-coded icon with relative severity value. See "System severity values," below.
Hostname	The Analyzer or Collector's user-assigned host name.
fps	The flows per second the Collector is sending to the Analyzer (or if the Analyzer is acting as a Collector, the flows per second it is collecting).
pps	The packets per second the Collector is sending to the Analyzer (or if the Analyzer is acting as a Collector, the packets per second it is collecting).
Uptime	The time that has elapsed since the appliance was last rebooted, in days, hours, and minutes.
Last Seen	The last time this Collector reported to the Analyzer.
Status	A system-generated message that describes the overall status of the appliance. See "Summary messages," below.
Flow sources	Lists the number of routers or interfaces the Collectors are collecting data from.
Version	The current software version each appliance is running.

Table 43: *System Status table*

Note: If an appliance is experiencing connectivity problems, Proventia Network ADS automatically displays that appliance's status information at the top of the page to immediately alert you. This prevents you from having to expand and scroll for information.

System severity values

Proventia Network ADS displays severity values and corresponding icons to indicate how the appliance is performing:

Severity Value	Icon Color and Shape	What it Indicates
1-3	Green triangle, pointing down	Your appliances are functioning correctly.
4-7	Yellow square	A problem is not severe but warrants investigation.
8-10	Red triangle, pointing up	A situation requires immediate attention.

Table 44: *System table severity values*

Status messages

Proventia Network ADS displays one of the following status messages:

- High memory usage: (*usage percentage*)
- Flow source (*name*) has problems
- High disk usage: (*amount of MB remaining*)
- Synchronize times: skew is (*amount of time*)
- Device is offline: last seen (*time last seen*)

- Multiple Problems: `(the list of problems)`
- Good

Chapter 17

Viewing Detail Pages

Overview

Introduction

The Summary, Explore, and Policy pages show you the most recent information for policy and system changes, but the Detail pages allow you to review entire logs at a greater level of detail.

In this chapter

This chapter contains the following topics:

Viewing Log Details

Introduction

The Log Detail pages show the logs of all change messages for system configuration or for a specific rule. System configuration changes include any changes made to a rule, group, port, time, or notification object.

Types of log entries

The type of log entries the system displays depends on how you navigate to the page. If you navigate from the Group Objects Configuration page (click the Full Change Log for Group Object link), the Log Detail page displays all group object changes. If you navigate from any other page, the system displays log messages that correspond to that page.

Example: If you click the log link from the Edit Port Groups page for your Windows port group, the system displays all change message log entries for only that port group.

Navigation and searching

Standard navigation and searching apply on all Detail pages.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Log detail tables

The Log Detail tables show different columns of information depending upon the log view. For the system, group, port, notification, and time object log views, the table displays the same information as the Recent Changes tables on their corresponding pages.

Reference: See "How Proventia Network ADS Determines Severity" on page 60 for a description of these columns.

To navigate to a corresponding Log Detail page, click the Full change log link on one of the following pages:

Page	Description
Edit Group Objects	The changes for the specific group object.
Policy	All the changes for all policy rules.
Event Details	All the changes for a specific policy rule.
Edit Notification Object	The changes for the specific notification object.
Edit Port Object	The changes for the specific port object.
Time Object	The changes for the specific time object.

Table 45: *Log pages*

Viewing Details for Hosts and Services

Introduction

You can navigate to the host or service log details from wherever a count of hosts or services is displayed in the Web user interface. These detail pages list all hosts and services represented by the summary row on the Explore page that matched your search. You can use this information in cleanup efforts following alert or attack activity.

Note: If the row displays an aggregate, this page displays only the members within the aggregate that match the traffic.

Example: If an aggregate contains 255 members, but only 17 of them matched the search you entered, the Explore page shows 17 in the Num column, and when you navigate to the host Details page, the information for those 17 hosts is displayed.

Searching on the host and services Details pages

You can filter the results shown by entering search values in the box.

Reference: For acceptable search formats, click the More link under the search box or see "About search values" on page 17

Host Detail page

The host Detail page shows a list of all affected or violating hosts (clients or servers). The page title describes the host view (for example, Detail for dest 10.0.1.1) and in some cases, identifies how you navigated to this page (the rule name). The Host Detail table shows the following for each listed host:

Column	Description
Client or Server	The host IP address and hostname (if known), and the info icon, which you can click to navigate to the entity Info page.
Groups	The names of all groups this host belongs to, with the info icon to navigate to additional views or information. **Reference:** See "Using info icons" on page 15.
Bytes	The amount of traffic flowing through this host.
Bps	The rate at which traffic is flowing through this host.

Table 46: *Host details table*

Making groups

To make groups from the hosts listed on the host Details page:

1. Select the host rows you want to include.
2. Type a name for the group object in the box.

   Note: Enter an existing name to add hosts to a group object.

   Reference: See "Naming group objects" on page 51.
3. Do one of the following:
   - Click NEW GROUP OBJECT.
   - Click MAKE GROUP FROM ALL to include all hosts listed on the page(s).

Service Detail page

The service Detail page provides a complete list of all services represented by the summary row on the Explore page. The page title describes the current view, which also shows the services you clicked on to navigate to this page. The table shows the service type along with all objects that cover the service.

Making port objects

To make port objects from the services listed on the service Details page:

1. Select the service rows you want to include.
2. Type a name for the group in the box.

   Note: Enter an existing name to add services to a port object.

   Reference: See "Naming port objects" on page 81.
3. Do one of the following:
   - Click **NEW PORT OBJECT**.
   - Click **MAKE PORT OBJECT FROM ALL** to include all services listed on the page(s).

Viewing Alert Details

Introduction

The Alert Detail page shows the details for all the violations that make up an alert summary row in the Alerts tables on the Event Details page.

The system displays three different types of Alert Detail pages:

- Traffic alert details for traffic violations, floods policies, and ATF policies.
- Port scan alert details for port scan behaviors.
- Host scan alert details for worms and host scan behaviors.

Navigation and searching

Standard navigation and searching apply on all Alert Detail pages. This includes using the links and icons that navigate and pivot the view of traffic data.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Types of information shown

The system displays different alert details in the table, depending upon the alert type. Some alert pages show traffic details with the severity, detail description, clients and servers, and the time the alert traffic was detected, and some only show affected targets.

About creating group objects on the Alert Details page

You can create new groups that include any or all of the clients or servers listed in the Alert Details table. Although you can create groups manually on the Group Object Configuration page, the groups you create on the Alert Details page show the traffic that hosts are involved in, so you can group them according to the way they behave.

Reference: See "Adding and Editing Group Objects" on page 51.

Using the selection check boxes

When creating groups, you must select the check boxes that appear next to the client or server, not the check boxes at the end of each row, as those apply to clearing or approving alerts, not to group creation. The Make Group from All button includes all hosts, including those that appear on additional pages.

Creating group objects

To create a group object:

1. Select the check boxes for all of the clients and servers you want to group together.
2. Enter a unique name for a new group in the text box.

   Note: Enter an existing name to add hosts to a group object.

   Reference: See "Naming group objects" on page 51.
3. Do one of the following:
   - Click **NEW GROUP OBJECT**.
   - Click **MAKE GROUP FROM ALL** to include all hosts listed on the page(s).

Showing traffic flows

You can see all of the traffic flows that contributed to this alert. Click the magnifying glass icon (or the View Flows link) to navigate to the Flows page where you can filter the results by searching for specific hosts or services.

Reference: See "Viewing Traffic Flows" on page 106.

About accepting alerts

Accept alert traffic listed in the Alerts table to update a rule. When you accept traffic, the system adds the traffic (client, server, service) to the list of acceptable traffic. ADS stops creating alerts when it sees future matching traffic.

When you select the check boxes at the end of alert rows and apply an action (clear alerts or approve), the system applies that action only to the selected rows on the current page. If you select the Select All check box (next to the Bytes column), the system applies the action to all rows on the current page.

Accepting alert traffic

To accept alert traffic:

1. Do one of the following:
   - Select the check box for each row that you want to include as acceptable behavior.
   - Select the Select All check box at the top of the table to include all rows on this page.
2. Click **ACCEPT**.

   The system updates the rule removes the alerts from the Event Details page.

Clearing alerts

You can clear alerts once you have determined they do not pose a threat to your network. If you clear an alert but do not update the rule, ADS generates alerts for any future violations of the rule that it detects.

To clear alerts:

1. Do one of the following:
   - Select the check box for the alert row that you want to remove.
   - Select the Select All check box at the top of the table to include all alerts on this page.
2. Click **CLEAR ALERTS**.

   The system removes the alerts from this page and from the Event Details page.

Exporting alert details

You can export the details from the table as a CSV file. Exporting this information can help you cleanup following a worm infection or other type of attack, or you can use this information for compliance auditing, or in reports. When you export alerts, the system includes all alerts from the table in the file, not just those on the current page.

To export the alert details:

1. Click **EXPORT**.
2. Specify how you want to save or open the file, according to the choices your browser displays.